

قرارداد نقطه به نقطه

این نوشتار به هیچ منبع و مرجعی استناد نمی‌کند.

[بیشتر بدانید](#)

پروتکل نقطه به نقطه (به انگلیسی: PPP) در شبکه‌های رایانه‌ای، پروتکل نقطه به نقطه (PPP) یک پروتکل ارتباطی لایه پیوند داده (لایه ۲) است که مستقیماً بین دو روتر (مسیریاب) بدون هیچ میزبان یا شبکه دیگری در این بین قرار دارد. می‌تواند تأیید اعتبار اتصال، رمزگذاری انتقال و فشرده‌سازی داده‌ها را فراهم کند.

PPP در بسیاری از انواع شبکه‌های فیزیکی از جمله کابل سریال، خط تلفن، خط ترانک، تلفن همراه، سیم‌های رادیویی تخصصی، ISDN، و سیم فیبر نوری مثل SONET (سلسه همگام رقمی) استفاده می‌شود. ارائه‌دهندگان خدمات اینترنتی (ISP) از PPP برای دسترسی شماره‌گیری به اینترنت استفاده کرده‌اند، بسته‌های IP نمی‌توانند بر روی یک خط مودم به تنهایی انتقال یابند، بدون یک پروتکل پیوند داده که بتواند جایی که بسته انتقال شروع شده و کجا به پایان می‌رسد را شناسایی شود.

دو مشتق PPP، پروتکل نقطه به نقطه بر روی اترنت (PPPoE) و پروتکل نقطه به نقطه بر روی (شبکه) حالت انتقال ناهمگام (PPPoA) که معمولاً توسط ISP ها برای یک خط مشترک دیجیتالی (DSL) برای اتصال سرویس اینترنت با مشتریان استفاده می‌شوند.

شرح

PPP معمولاً به عنوان یک پروتکل لایه پیوند داده برای اتصال از طریق مدارهای همزمان و ناهمزمان مورد استفاده قرار می‌گیرد، جایی که تا حد زیادی جایگزین پروتکل اینترنت سری قبلی (SLIP) و استانداردهای اجباری شرکت تلفنی شده (مانند پروتکل دسترسی به لینک متوازن (LAPB) در مجموعه پروتکل X.25) است. تنها نیاز PPP این است که مدار ارائه شده باید دو طرفه باشد. PPP برای کار با پروتکل‌های لایه شبکه متعددی از جمله پروتکل اینترنت (TRILL), (IP), تبادل بسته بین شبکه‌ای (NBF DECnet), (IPX) و AppleTalk طراحی شده است. مانند SLIP که یک اتصال کامل اینترنتی روی

خطوط تلفن از طریق مودم است. قابل اطمینان تر از SLIP است زیرا برای اطمینان از سالم بودن بسته های اینترنت آن را دو بار بررسی می کند. بسته های آسیب دیده را دوباره ارسال می کند.

PPP تا حدی بعد از ویژگی های اصلی HDLC طراحی شد. طراحی های PPP ویژگی های اضافی دیگری را شامل می شوند که تا آن زمان فقط در پروتکل های پیوند داده اختصاصی مشاهده شده بودند. PPP در RFC 1661 مشخص شده است.

RFC 2516 پروتکل نقطه به نقطه روی اترنت (PPPoE) را به عنوان روشی برای انتقال PPP روی اترنت توصیف می کند که گاهی با DSL استفاده می شود.

۲۳۶۴ پروتکل نقطه به نقطه را بر روی (ATM (PPPoA) به عنوان روشی برای انتقال PPP از طریق لایه ۵ سازگاری با دستگاه (ATM (AAL5) توصیف می کند، که همچنین یک جایگزین دیگر برای PPPoE استفاده شده با DSL است.

PPP, PPPoE و PPPoA به طور گسترده ای در خطوط WAN استفاده می شود.

PPP یک پروتکل لایه ای است که دارای سه جز است:

1. یک جز کپسوله شده که برای انتقال داده ها از روی لایه فیزیکی مشخص استفاده می شود.
2. یک پروتکل کنترل پیوند (LCP) برای ایجاد، پیکربندی و آزمایش پیوند و همچنین مذاکره درباره تنظیمات، گزینه ها و استفاده از ویژگی ها.
3. یک یا چند پروتکل کنترل شبکه (NCP) برای مذاکره در مورد پارامترهای پیکربندی اختیاری و امکانات لایه شبکه استفاده می شود. برای هر پروتکل لایه بالاتر یک NCP وجود دارد که توسط PPP پشتیبانی می شود.

پیکربندی خودکار

LCP ارتباطات را با ظرافت آغاز و خاتمه می دهد، به میزبان اجازه می دهد تا در مورد گزینه های اتصال تبادل کند. این بخش جدایی ناپذیر از PPP است و با همان مشخصات استاندارد تعریف می شود. LCP پیکربندی اتوماتیک واسطها در هر انتها (مانند تنظیم اندازه دیتاگرام، نویسه های فرار شده و اعداد جادویی) و برای انتخاب احراز هویت اختیاری فراهم می کند. پروتکل LCP در بالای PPP (با شماره پروتکل PPP 0xc021) اجرا می شود و بنابراین قبل از اینکه LCP بتواند آن را پیکربندی کند باید یک اتصال بنیادی PPP برقرار شود.

RFC 1994 پروتکل تایید هویت دست دادن (CHAP) را توصیف می کند، که برای برقراری ارتباط شماره گیری با ISP ترجیح داده می شود. اگرچه منسوخ شده است، اما پروتکل احراز هویت رمز عبور (PAP) هنوز هم گاهی اوقات استفاده می شود.

گزینه دیگر برای احراز هویت از طریق PPP، پروتکل احراز هویت قابل توسعه (EAP) است که در RFC 2284 شرح داده شده است. پس از ایجاد پیوند، ممکن است پیکربندی شبکه (لایه ۳) اضافی رخ دهد. به طور معمول، پروتکل کنترل پروتکل اینترنت (IPCP) استفاده می شود، هر چند پروتکل کنترل تبادل بسته اینترنت (IPXCP) و پروتکل کنترل

AppleTalk (ATCP) زمانی محبوب بودند پروتکل کنترل نسخه ۶ پروتکل اینترنت (IPv6CP) استفاده گسترده در آینده را مشاهده خواهد کرد، زمانی که IPv6 جایگزین IPv4 را به عنوان پروتکل لایه ۳ جایگزین می‌کند.

پروتکل‌های لایه شبکه چندگانه

PPP به چندین پروتکل لایه شبکه اجازه می‌دهد تا روی همان پیوند ارتباطی کار کنند. برای هر پروتکل لایه شبکه، یک پروتکل کنترل شبکه جداگانه (NCP) به منظور کپسوله سازی و تبادل گزینه‌های برای پروتکل‌های لایه شبکه چندگانه ارائه شده‌است. با اطلاعات لایه شبکه تبادل می‌کند، به عنوان مثال آدرس شبکه یا گزینه‌های [فشرده سازی](#)، پس از برقراری اتصال.

به عنوان مثال، پروتکل اینترنت (IP) از پروتکل کنترل (IPCP) (IP) و تبادل بسته‌های اینترنت (IPX) از پروتکل کنترل (Novell IPX (IPX / SPX استفاده می‌کند.

NCP های زیر ممکن است با PPP استفاده شوند:

- پروتکل کنترل پروتکل اینترنت (IPCP) برای IP، به شماره پروتکل x8021
[RFC 1332](#)
- پروتکل کنترل کننده ی لایه شبکه (OSI (OSINLCP) برای پروتکل های مختلف لایه شبکه [OSI](#)، به شماره پروتکل x8023
[RFC 1377](#)
- پروتکل کنترل (AppleTalk (ATCP) برای AppleTalk، به شماره پروتکل x8029
[RFC 1378](#)
- پروتکل کنترل تبادل بسته اینترنت (IPXCP) برای تبادل بسته اینترنت، به شماره پروتکل x802B
[RFC 1552](#)
- پروتکل کنترل (IV فاز DNCP) (DECnet (DNCP) برای پروتکل مسیریابی IV فاز DNA، به شماره پروتکل x8027
[RFC 1762](#)
- پروتکل کنترل فریم های (NetBIOS (NBFCP) برای پروتکل Frames NetBIOS (یا همان NetBEUI که قبلاً نامیده می‌شد)، به شماره پروتکل x803F
[RFC 2097](#)
- پروتکل کنترل (IPv6 (IPV6CP) (IPv6) برای IPv6، به شماره پروتکل x8057
[RFC 5072](#)

تشخیص پیوند حلقه ای

PPP ارتباطات را با استفاده از یک ویژگی شامل اعداد جادویی شناسایی می‌کند. زمانی که گره پیام‌های LCP را ارسال می‌کند، این پیام‌ها ممکن است شامل یک عدد جادویی باشند. اگر یک خط حلقه گردد، گره پیام LCP را با عدد جادویی خود دریافت می‌کند، به جای آن که یک پیام با شماره جادویی همتای خود دریافت کند.

گزینه های پیکربندی

در بخش قبلی استفاده از گزینه های LCP برای تأمین نیازهای خاص اتصال WAN معرفی شده است. PPP ممکن است شامل گزینه های LCP زیر باشد:

- **احراز هویت**

روتراهی همتا پیام های احراز هویت را رد و بدل می کنند. دو گزینه احراز هویت عبارتند از: پروتکل تأیید گذرواژه (PAP) و پروتکل چالش - دست‌دهی تأیید هویت (CHAP). احراز هویت در بخش بعدی توضیح داده شده است.

- **فشرده سازی**

با کاهش مقدار داده در فریم که باید از طریق پیوند عبور کند، توان موثر در اتصالات PPP را افزایش می دهد. پروتکل فریم را در مقصد از حالت فشرده خارج می کند. برای جزئیات بیشتر به [RFC 1962](#) مراجعه کنید.

- **تشخیص خطا**

شرایط خطا را شناسایی می کند. گزینه های کیفیت و اعداد جادویی به اطمینان از پیوند داده ای مطمئن و بدون حلقه کمک می کنند. قسمت اعداد جادویی در تشخیص پیوندهایی که در وضعیت بازگشتی هستند کمک می کند. تا زمانی که گزینه پیکربندی اعداد جادویی با موفقیت تبادل شود، اعداد جادویی باید به صفر منتقل شود. اعداد جادویی به طور تصادفی در هر انتهای اتصال تولید می شوند.

- **چند منظوره**

تعداد بار چندین رابط مورد استفاده توسط PPP از طریق PPP چند منظوره را فراهم می کند.

فریم PPP

فریم های PPP انواع فریم های HDLC هستند:

نام	تعداد بایت ها	شرح
پرچم	۱	0x7E, ابتدای یک قاب PPP
آدرس	۱	0xFF, آدرس پخش استاندارد
کنترل	۱	0x03, داده های بدون شماره
پروتکل	۲	شناسه PPP داده های جاسازی شده
اطلاعات	متغیر (۰ یا بیشتر)	دیتاگرام
لایه گذاری	متغیر (۰ یا بیشتر)	لایه اختیاری
توالی بررسی فریم	۲	مجموع کنترل قاب
پرچم	۱	0x7E, برای بسته های پی در پی PPP حذف شده است

اگر هر دو طرف بر روی فشردگی میدان و کنترل میدان در طول LCP توافق کنند، آنگاه این قسمت ها حذف می شوند. همچنین اگر هر دو طرف با فشردگی میدان پروتکل توافق کنند، آنگاه بایت 0X00 را می توان حذف کرد.

قسمت پروتکل نوع بسته انتقالی را نشان می دهد: 0xC021 برای 0x80xy LCP، برای NCPs مختلف، 0x0021 برای NetBIOS، 0x002B Apple Talk، 0x0029 IP، 0x003D برای IPX، برای چند منظوره، 0x003F برای 0x00FD NetBIOS، برای MPPE و MPPC و غیره. PPP برخلاف EtherType محدود است و نمی تواند شامل داده های عمومی لایه ۳ باشد.

قسمت اطلاعات شامل بسته انتقالی PPP است. دارای تغییری است با اندازه ی حداکثر انتقال که **بیشینه واحد انتقال** نام دارد. به طور پیش فرض، حداکثر ۱۵۰۰ **هشت تایی** است. ممکن است روی انتقال پد شود. اگر اطلاعات مربوط به یک پروتکل خاص بتواند پد شود، این پروتکل باید اجازه دهد اطلاعات از پد متمایز شود.

کپسوله سازی

فریم های PPP در یک پروتکل لایه پایین تر کپسوله می شوند که قاب بندی را فراهم می کند و ممکن است توابع دیگری مانند یک **جمع آزمون** برای تشخیص خطاهای انتقال را فراهم کند. PPP در پیوندهای سریال معمولاً در قاب مشابه HDLC، که توسط **RFC 1662 IETF** توصیف می شود، کپسوله می شود.

نام	تعداد بایت ها	شرح
پرچم	۱	شروع یا پایان قاب را نشان می دهد
آدرس	۱	آدرس پخش
کنترل	۱	کنترل بایت
پروتکل	۱ یا ۲ یا ۳	در زمینه اطلاعات
اطلاعات	متغیر (۰ یا بیشتر)	دیتاگرام
لایه	متغیر (۰ یا بیشتر)	لایه اختیاری
FCS	۲ یا ۴	بررسی خطا

فیلد Flag در صورت استفاده از PPP با کادر بندی HDLC مانند وجود دارد.

قسمتهای آدرس و کنترل همیشه دارای مقدار hex FF (برای "همه ایستگاه ها") و hex 03 (برای "اطلاعات بدون شماره") هستند ، و هر زمان که PPP LCP آدرس-و-کنترل-زمینه-فشرده سازی (ACFC) تبادل می شود می تواند حذف شود .

قسمت تعیین توالی قاب (FCS) برای تعیین خطای یک فریم منفرد استفاده می شود. این شامل یک جمع‌آزما محاسبه شده بر روی قاب برای محافظت اساسی در برابر خطاهای انتقال است. این یک کد CRC مشابه کدی است که برای سایر طرح های محافظت از خطای پروتکل لایه دیگر مانند آنچه در اترنت استفاده شده است. براساس RFC 1662 ، این اندازه می تواند ۱۶ بیت (۲ بایت) یا ۳۲ بیت (۴ بایت) باشد (پیش فرض ۱۶ بیت است - چند جمله ای FCS). $x^{16} + x^{12} + x^5 + 1$ پس از کپسوله شدن پیام بر روی قسمتهای آدرس ، کنترل ، پروتکل ، اطلاعات و پدینگ محاسبه می شود.

فعال سازی خط و فازها

- پیوند مرده

این مرحله زمانی رخ می دهد که پیوند از کار بیفتد یا به یک طرف گفته شود که قطع شود (به عنوان مثال کاربر شماره گیری خود را به پایان رسانده است).

- مرحله ایجاد پیوند

این مرحله جایی است که مذاکرات پروتکل کنترل پیوند انجام می شود. در صورت موفقیت ، کنترل به فاز تایید یا فاز پروتکل لایه - لایه می رود بسته به اینکه آیا احراز هویت مورد نظر است یا خیر.

- مرحله احراز هویت

این مرحله اختیاری است. به طرفین اجازه می دهد قبل از برقراری ارتباط ، یکدیگر را احراز هویت کنند. در صورت موفقیت ، کنترل به مرحله پروتکل لایه شبکه می رود.

- مرحله پروتکل لایه شبکه

این فاز جایی است که هر کدام از پروتکل‌های کنترل شبکه مورد نظر فراخوانی می‌شوند. به عنوان مثال، IPCP در ایجاد سرویس IP از طریق خط استفاده می‌شود. انتقال داده برای تمام پروتکل‌هایی که با موفقیت با پروتکل‌های کنترل شبکه خود شروع می‌شوند نیز در این مرحله اتفاق می‌افتد. بسته شدن پروتکل‌های شبکه نیز در این مرحله اتفاق می‌افتد.

- **مرحله خاتمه پیوند**

این مرحله این اتصال را قطع می‌کند. اگر خطای تأیید اعتبار وجود داشته باشد، اگر اشتباهات مجموع زیادی در کنترل وجود داشته باشد، دو طرف تصمیم می‌گیرند پیوند را به طور خودکار از بین ببرند، اگر پیوند ناگهان خراب شود، یا اگر کاربر تصمیم به قطع اتصال داشته باشد، این اتفاق می‌افتد.

از طریق چندین لینک

PPP چند منظوره

PPP چند منظوره (که به آن MLP, MPPP, MP, MLPPP یا چند منظوره نیز گفته می‌شود) روشی را برای پخش ترافیک در چندین اتصال مشخص PPP ارائه می‌دهد. این مورد در [RFC 1990](#) تعریف شده است. می‌توان از آن برای مثال برای اتصال کامپیوتر خانگی به یک سرویس دهنده اینترنت با استفاده از دو مودم سنتی 56k یا برای اتصال یک شرکت از طریق دو خط اجاره ای استفاده کرد.

در یک خط PPP فریم‌ها نمی‌توانند از حالت خارج خارج شوند، اما این امکان وجود دارد که فریم‌ها بین چندین اتصال PPP تقسیم شوند. بنابراین، PPP چندمنظوره باید قطعات را شماره گذاری کند تا هنگام ورود مجدداً آنها را به ترتیب صحیح قرار داد. PPP چند منظوره مثالی از فناوری تجمیع پیوند است. [Cisco IOS](#) نسخه ۱۱٫۱ را منتشر می‌کند و بعداً از PPP چند منظوره پشتیبانی می‌کند.

PPP چند کلاسه

با PPP، نمی‌توان چندین اتصال PPP متمایز همزمان را از طریق یک پیوند برقرار کرد. این کار با PPP چند منظوره نیز امکان پذیر نیست.

PPP چند منظوره برای همه قطعات یک بسته از اعداد مجاور استفاده می‌کند و در نتیجه امکان ارسال توالی قطعات یک بسته به منظور ارسال بسته دیگر وجود ندارد. با این کار چندین بار PPP چند منظوره روی پیوندهای مشابه اجرا نمی‌شود.

PPP چند کلاسه نوعی PPP چند منظوره است که در آن هر "کلاس" از ترافیک از فضای عددی توالی جداگانه و بافر جمع آوری مجدد استفاده می‌کند. PPP چند کلاسه در [RFC 2686](#) تعریف شده است.

تونل ها

پروتکل های مشتق شده

PPTP (قرارداد تونل زنی نقطه به نقطه) نوعی PPP بین دو میزبان از طریق GRE با استفاده از رمزگذاری (MPPE) و فشرده سازی (MPPC) است.

به عنوان یک قرارداد ۲ لایه بین دو انتهای تونل

از پروتکل های بسیاری می توان برای تونل سازی داده ها از طریق شبکه های IP استفاده کرد. برخی از آنها مانند SSL, SSH یا L2TP رابط های شبکه مجازی ایجاد می کنند و تصور اتصال مستقیم فیزیکی بین نقاط انتهایی تونل را ایجاد می کنند. به عنوان مثال در یک میزبان Linux, این رابط ها tun0 یا ppp0 نامیده می شوند.

از آنجا که فقط دو نقطه انتهایی در یک تونل وجود دارد, تونل یک اتصال نقطه به نقطه است و PPP یک انتخاب طبیعی به عنوان پروتکل لایه پیوند داده بین رابط های شبکه مجازی است. PPP می تواند آدرس های IP را به این رابط های مجازی اختصاص دهد و از این آدرس های IP می توان برای مسیریابی بین شبکه های دو طرف تونل استفاده کرد.

IPsec در حالت تونل سازی رابط های فیزیکی مجازی را در انتهای تونل ایجاد نمی کند, زیرا تونل مستقیماً توسط پشته TCP / IP اداره می شود. برای تهیه این رابط ها می توان از L2TP استفاده کرد, این روش L2TP / IPsec نامیده می شود. در این مورد نیز PPP آدرس های IP را به قسمت انتهایی تونل ارائه می دهد.

استانداردهای IETF

PPP در RFC 1661 (پروتکل نقطه به نقطه, ژوئیه ۱۹۹۴) تعریف شده است. RFC 1547 (الزامات پروتکل استاندارد به نقطه از نقطه به نقطه در اینترنت, دسامبر ۱۹۹۳) اطلاعات تاریخی درباره نیاز به PPP و توسعه آن را ارائه می دهد. یک سری RFC های مرتبط برای تعریف نحوه کار پروتکل های مختلف کنترل شبکه از جمله TCP / IP, DECnet, AppleTalk, IPX و سایر موارد با PPP نوشته شده است.

- (RFC 1332, The PPP Internet Protocol Control Protocol (IPCP
- (RFC 1661, Standard 51, The Point-to-Point Protocol (PPP
- RFC 1662, Standard 51, PPP in HDLC-like Framing
- (RFC 1962, PPP Compression Control Protocol (CCP
- RFC 1963, PPP Serial Data transport Protocol

- [RFC 1877](#), PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
- ([RFC 1990](#), The PPP Multilink Protocol (MP
- ([RFC 1994](#), PPP Challenge Handshake Authentication Protocol (CHAP
- [RFC 2153](#), Informational, PPP Vendor Extensions
- ([RFC 2284](#), PPP Extensible Authentication Protocol (EAP
- [RFC 2364](#), PPP over ATM
- [RFC 2516](#), PPP over Ethernet
- [RFC 2615](#), PPP over SONET/SDH
- [RFC 2686](#), The Multi-Class Extension to Multi-Link PPP
- [RFC 2687](#), Proposed Standard, PPP in a Real-time Oriented HDLC-like Framing
- [RFC 5072](#), IP Version 6 over PPP
- [RFC 5172](#), Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol
- [RFC 6361](#), PPP Transparent Interconnection of Lots of Links ([TRILL](#)) Protocol Control Protocol
- :Additional drafts
- PPP Internet Protocol Control Protocol Extensions for IP Subnet (draft) (<https://tools.ietf.org/html/draft-helenius-ppp-subnet-00>)
- PPP IPV6 Control Protocol Extensions for DNS Server Addresses (draft) (<https://tools.ietf.org/html/draft-ietf-pppext-ipv6-dns-addr-03>)
- PPP Internet Protocol Control Protocol Extensions for Route Table Entries (draft) (<https://tools.ietf.org/html/draft-kehn-info-ppp-ipcp-ext-00>)
- PPP Consistent Overhead Byte Stuffing (draft) (<https://tools.ietf.org/html/draft-ietf-pppext-co>) ([bs-00](#)) (cf. Consistent Overhead Byte Stuffing

جستارهای وابسته

- قرارداد تونل‌زنی نقطه‌به‌نقطه
- حالت انتقال ناهمگام

منابع

برگرفته از «https://fa.wikipedia.org/w/index.php?title=قرارداد_نقطه_به_نقطه&oldid=33440723»

آخرین ویرایش ۱ سال پیش توسط HujiBot انجام شده

ویکی‌پدیا
